Come determinare la Cybersecurity Posture: i security assessment

Introduzione

In un contesto in cui la **digitalizzazione** sta crescendo costantemente, è importante sapere come sfruttare gli strumenti che ci offre, ma anche come proteggerci dalle minacce che può comportare. Questo articolo si concentra sulla determinazione della **Cybersecurity Posture** e sui **Security Assesment**, fornendo informazioni utili per comprendere il loro attuale livello di rischio e stabilire una strategia per proteggersi dagli attacchi informatici e quindi migliorare la propria sicurezza.

Per Cybersecurity Posture si intende lo stato di sicurezza di un'organizzazione, in funzione delle sue politiche di gestione di software, hardware e dati, e la sua capacità di difendersi e reagire agli attacchi informatici.

Determinare la Cybersecurity Posture permette ad una organizzazione di comprendere le azioni da introdurre in ambito organizzativo, formativo e tecnologico per far fronte alla costante crescita dei tentativi di compromissione, esfiltrazione dati o estorsione (ransomware). È fondamentale, infatti, non essere impreparati alla continua evoluzione delle metodologie e del numero di tentativi di accessi non autorizzati alle risorse aziendali, sia da parte di soggetti esterni all'organizzazione sia da parte di quelli interni.

Per determinare la Cybersecurity Posture di una organizzazione è necessario raccogliere diverse informazioni, di carattere sia organizzativo che tecnico, attraverso una attività di **Cybersecurity Assesment** (o security assessment). Non esiste

una metodologia unica per determinare la Cybersecurity Posture, e sono possibili diversi approcci e scale di valutazione. Questo può rappresentare un elemento di confusione per le organizzazioni, che non riescono a determinare come procedere o a quale metodologia affidarsi.

Un Cybersecurity Assessment (brevemente CSA) è un processo di analisi che valuta un'organizzazione e la sua capacità di rilevare e gestire attacchi informatici, o le loro conseguenze. Per questo il Cybersecurity Assessment deve tenere in considerazione differenti aspetti:

1. l'identificazione degli asset e dei servizi da proteggere, in particolare quelli critici;
2. la valutazione degli strumenti di protezione e monitoring in uso;
3. la disponibilità di processi per la gestione degli espetti di sicurezza (prevenzione, reazione, documentazione, etc,);
4. il livello di sensibilità e competenza del personale sui temi della sicurezza.

I principali *framework* che stabiliscono come per svolgere un Cybersecurity Assessment includono:

- **NIST Cybersecurity Framework**: sviluppato dall'Istituto Nazionale degli Standard e della Tecnologia degli Stati Uniti, è uno dei framework più conosciuti. Fornisce linee guida per aiutare le organizzazioni a gestire e ridurre i rischi di cybersecurity;
- **ISO/IEC 27000 series**: questa serie di standard internazionali è focalizzata sulla sicurezza delle informazioni e offre un modello per l'implementazione, il monitoraggio e il miglioramento di un sistema di gestione della sicurezza delle informazioni;
- **CIS Critical Security Controls:** sono controlli di sicurezza sviluppati a partire dal 2008 dal consorzio CIS (Center for Internet Security) che, a livello

internazionale, riunisce aziende, agenzie governative, istituzioni e individui provenienti da ogni parte dell'ecosistema informatico. Contengono una serie di azioni raccomandate per la difesa informatica che forniscono modi specifici, e attuabili, per contrastare gli attacchi più pervasivi;
- **Framework Nazionale per la Cybersecurity e la Data Protection**: Questo framework è specifico per l'Italia e fornisce una metodologia per valutare la postura di cybersecurity delle organizzazioni nel contesto nazionale.

Impresoft 4ward, per erogare ai propri Clienti il Cybersecurity Assessment, ha scelto di utilizzare come principale riferimento il framework del CIS (Center for Internet Security): di carattere internazionale, non collegato ad alcuna organizzazione specifica e, soprattutto, dotato di **elementi pragmatici** che consentono la rapida determinazione di un piano **di azione** che possa indirizzare con efficacia i propri Clienti ad affrontare gli elementi manchevoli rilevati.

I principali fattori che influenzano la Cybersecurity Posture

Molte organizzazioni, purtroppo, tendono ancora a declinare la valutazione delle Cybersecurity Posture sul fronte esclusivamente tecnologico attuando solamente alcuni tipi di assessment di sicurezza, indubbiamente utili, ma non sufficienti da soli per la determinazione delle Cybersecurity Posture. Sono fondamentali, infatti, nella strategia di sicurezza aziendale, gli aspetti organizzativi con i quali l'organizzazione deve fronteggiare il rischio, tra questi ricordiamo:

- valutazione periodica del rischio informatico;
- coinvolgimento del top Management nelle decisioni relative alle strategia di sicurezza;
- definizione e mantenimento di politiche aziendali di sicurezza tra cui:

- ruoli e responsabilità;
- accesso sicuro alle risorse aziendali e uso dei dispositivi personali;
- condivisione delle informazioni aziendali;
- classificazione e protezione dei dati;
- risposta agli incidenti di sicurezza;
- qualifica di sicurezza dei software aziendali;
- qualifica di sicurezza per Partner e fornitori.
- formazione e cybersecurity awareness;

Per completezza riepiloghiamo comunque, a seguire, alcune tipologie di security assessment e i loro effettivi obiettivi.

Vulnerability Assessment (VA)

È un processo di analisi, svolto tramite **strumenti software specifici**, per l'identificazione e classificazione di vulnerabilità note, presenti nel software (o firmware) dei sistemi collegati alla rete aziendale.

Un vulnerabilità software corrisponde alla possibilità (presunta o reale) per un attaccante di sfruttare una specifica condizione di un sistema per ottenere informazioni, o svolgere azioni, in modo non autorizzato. Le vulnerabilità possono consistere in:

- errori del software/firmware (bug) dei sistemi;
- errori umani nella configurazione del sistema operativo, delle applicazioni o dei servizi;
- inadeguatezza della configurazione del sistema operativo, delle applicazioni o dei servizi (es: configurazioni di default);
- assenza di strumenti di protezione specifici;
- obsolescenza delle soluzioni software o degli strumenti di protezione.

La valutazione della **gravità** delle vulnerabilità di norma viene quantificata tramite il sistema Common Vulnerability Scoring System (CVSS) o altri sistemi proprietari collegati

agli strumenti che svolgono la valutazione (es. in scala Low/Medium/High, oppure con altre scale numeriche).

L'obiettivo dell'attività di Vulnerability Assessment è identificare la presenza delle vulnerabilità nei sistemi dell'organizzazione analizzati, allo scopo di eliminarle o mitigarle tramite le attività di *remediation*. Rimediare ad una vulnerabilità dipende dalla natura delle vulnerabilità stessa. Genericamente parlando è comunque possibile indentificare le principali categorie di remediation con:

- **software updating (o patching)** – attività di distribuzione e installazione di aggiornamenti software dell'applicazione/servizio vulnerabile allo scopo di sostituire la parte di codice che contiene la vulnerabilità, con un nuovo codice corretto;
- **software upgrading** – attività di distribuzione e installazione di una nuova versione dell'applicazione/servizio vulnerabile che non contiene più la vulnerabilità;
- **configuration change** – attività di modifica delle configurazione del sistema, applicazione o servizio, al fine di evitare o mitigare lo sfruttamento della vulnerabilità.
- **decommissioning** – attività che prevedere la rimozione del sistema, applicazione o servizio, in modo da eliminare la presenza della vulnerabilità.

Tramite le *remediation* le vulnerabilità possono essere risolte o mitigate. Per mitigate si intende l'effetto di ridurre, senza poter annullare, la possibilità che la vulnerabilità sia sfruttata dall'attaccante, o degli effetti a cui questo sfruttamento potrebbe portare. In assenza di possibilità di risoluzione o mitigazione talvolta risulta necessario accettare la presenza della vulnerabilità adottando misure esterne all'applicazione o al servizio oggetto della vulnerabilità (si pensi ad esempio al caso di applicazioni o sistemi operativi non più supportati dal relativo vendor).

È importante inoltre sottolineare che l'attività di *Vulnerability Assessment* (VA) si differenzia dal *Vulnerability Management* (VM). Questa infatti prevede, oltre all'attività di VA, anche l'analisi degli **impatti** delle remediation e il relativo **piano di adozione**. Il Vulnerability Management, inoltre, prevedere un processo continuo di VA ripetuto nel tempo, secondo uno schema pianificato e costante. Il Vulnerability Management, quindi, è una forma più organizzata e completa del VA, come processo ciclico e continuativo per identificare, classificare, rimediare e mitigare le vulnerabilità ed è spesso collegato ad un processo di *asset* discovery e *asset management*.

Penetration Test (PT)

È il processo operativo di analisi e valutazione della sicurezza di un sistema informatico condotto da una **persona** (Penetration tester o Ethical hacker) attraverso l'uso del suo ingegno e strumenti di sua scelta (hacking tools). In genere viene eseguito senza che la persona conosca informazioni sull'infrastruttura IT oggetto della verifica (*Black Box PT*). E' possibile tuttavia svolgere Penetration Test anche in modalità *White box*, quando vengono fornite conoscenze dettagliate dell'infrastruttura da esaminare, o *Grey box* quando vengono fornite al Penetration Tester solo alcune informazioni dell'infrastruttura da esaminare. L'attività del soggetto che svolge il Penetration Test può prevedere anche tecniche non tecnologiche come il *Social Engineering* per ottenere una parte delle informazioni necessarie al suo scopo.

L'obiettivo del Penetration Test è dimostrare di poter superare i sistemi di protezione del sistema informatico aziendale per compromettere l'organizzazione, sfruttando l'eventuale presenza di vulnerabilità, errori di configurazione, o la mancanza di protezione di alcuni sistemi o dati.

Questa modalità riflette le modalità operative, e le tecniche,

utilizzate dai reali soggetti attaccanti e richiede quindi una notevole competenza analoga degli strumenti e delle procedure utilizzate.

Breach and Attack Simulation (BAS)

Questo tipo di security assessment utilizza strumenti per l'**automazione di procedure** che utilizzano tecniche di attacco note riproducendone il comportamento. Lo scopo di questa metodologia è quella di valutare costantemente, nell'insieme, gli strumenti di sicurezza in uso dall'organizzazione e di verificarne quindi l'efficacia. Con questi strumenti è possibile, ad esempio, verificare l'efficacia dei sistemi anti-phishing della posta elettronica, o dei sistemi EDR/XDR di cui l'organizzazione è dotata. Anche il personale può essere oggetto di verifica da parte di questi strumenti attraverso, ad esempio, campagne di phishing simulato che hanno l'obiettivo di verificare se i continui processi formativi di *cybersecurity awareness*, adottati dall'organizzazione per il proprio personale, sono efficaci.

Security assessment specifici

È possibile anche declinare dei security assessment a specifici ambiti in modo più verticale, al fine di valutare il livello di rischio, e le possibili *remedaition*, di uno specifico servizio o insieme di servizi. L'obiettivo di questi assessment verticali è focalizzare l'attenzione su uno specifico ambito, per rilevare vulnerabilità o mancanze allo scopo di ridurre la superficie di attacco, migliorando la configurazione del servizio e/o adottando soluzioni di protezione specifiche. Ad esempio, è possibile svolgere attività di assessment di sicurezza specifici nei seguenti ambiti:

- l'identity provider e sistema di autenticazione on-premise o cloud;
- i servizi di produttività e collaborazione;

- i dispositivi e i relativi software utilizzati dagli utenti;
- la piattaforma di business intelligence;
- i servizi IaaS, PaaS e SaaS in cloud;

Ognuna di queste attività è utile all'organizzazione per contribuire dal punto di vista **tecnico** al miglioramento della sicurezza, tuttavia, non affrontano gli aspetti **organizzativi** e **formativi** come il Cybersecurity Assessment.

Conclusioni

Ognuno dei security assessment riportati in precedenza apporta un contributo al miglioramento della Cybersecurity Posture, tuttavia, alcuni di essi valutano solamente aspetti tecnologici e non affrontano in modo completo le tematiche della sicurezza dell'organizzazione anche dal punto di vista organizzativo. Possiamo rappresentare, in questo senso, nello schema seguente le varie soluzioni in precedenza descritte secondo i fattori di complessità e completezza dell'analisi:



È importante valutare, infatti, questi due aspetti dei vari security assessment per comprendere quale valore essi possano apportare alla determinazione delle Cybersecurity Posture.

Altri fattori da considerare per la messa in opera dei security assesment sono anche la **frequenza di attuazione** e l'eventuale possibile **impatto** sull'operatività dei servizi. Ogni security assessment, infatti, diventa obsoleto poco dopo essere stato svolto. La rapidità con cui sono individuate e sfruttate nuove vulnerabilità software e definite nuove tecniche di attacco o esfiltrazione dati (sommata all'evoluzione dei prodotti stessi), richiede di rivalutare periodicamente gli aspetti tecnici. È da considerare invece che, sul fronte organizzativo, per attuare reali cambiamenti a livello di politiche e processi di gestione spesso è

necessario tempo.

Rivalutare periodicamente la Cybersecurity Posture o lo stato di sicurezza di uno specifico ambito serve comunque a misurare i progressi ottenuti e stabilire quindi il miglioramento dello stato di sicurezza della propria organizzazione.

Si consiglia di effettuare un Cybersecurity Assessment ogni anno, mentre per il Vulnerability Assessment si può prevedere una frequenza trimestrale o semestrale. La frequenza per altri security assessment più specifici va valutata in funzione della tecnologia utilizzata e al suo livello di criticità ed evoluzione all'interno dell'organizzazione.

Ad esclusione del Penetration Test che potrebbe, in funzione degli strumenti utilizzati, generare una possibile impatto funzionale, di norma le altre tipologie di assessment corrispondono in genere ad una raccolta di informazioni dai sistemi oggetto dell'analisi e/o dal personale IT, e quindi non prevedono un impatto sui sistemi analizzati.

Impresoft 4ward forte della propria esperienza sul fronte della sicurezza può aiutarti a determinare la Cybersecurity Posture della tua organizzazione o effettuare attività di security assessment specifici per migliorare la sicurezza dei tuoi servizi. Contattaci per raccontarci le tue necessità e definire la migliore soluzione alle tue esigenze.

Vuoi saperne di più?

Scopri subito come vincere la sfida al cambiamento

Contatta subito Impresoft 4ward

Articolo a cura di **Davide Bertarelli**

Profilo Autore

Nel corso degli ultimi trent'anni ha svolto attività di sviluppo software, system administration, consulente, team

leader e trainer.
Microsoft Cybersecurity Architect e Microsoft Certified Trainer ha svolto attività divulgativa, di formazione, e consulenziale per diverse tecnologie, per aziende a carattere nazionale e internazionale.
Negli ultimi cinque anni ha focalizzato le proprie energie nell’ambito della Cybersecurity per accompagnare aziende e organizzazioni, in sicurezza, nella loro trasformazione digitale.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/come-determinare-la-cybersecurity-posture-i-security-assessment/